

WRITTEN TESTIMONY
FOR THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
TOM DAVIS, CHAIRMAN (VIRGINIA)
HENRY WAXMAN, RANKING MINORITY MEMBER (CALIFORNIA)

INVESTIGATIVE HEARING ON PRIVACY AND SECURITY WITH REGARD TO
PEER TO PEER FILE SHARING

HEARING DATE: MAY 15, 2003 10:00 A.M.

ROOM 2154

RAYBURN HOUSE OFFICE BUILDING

TESTIMONY PROVIDED BY MARI J. FRANK, ESQ.

Good morning, Chairman Davis, Ranking Member Waxman, honorable committee members, and invited guests. Thank you very much for the opportunity to address you today regarding privacy and security with reference to the possible vulnerabilities of computer users when engaged in peer to peer file sharing on the Internet. I am also very grateful that Congress is looking at the greater issue of identity theft to understand how it fits into the overall issue of privacy and security in our society.

My name is Mari Frank. I am an attorney, privacy and identity theft consultant, and author of The Identity Theft Survival Kit, (Porpoise Press) and co-author of Privacy Piracy (Office Depot) from Laguna Niguel, California. I serve as a Sheriff Reserve for the Orange County, California Sheriff Department's High Tech Crime Unit, and sit on the Advisory Committee to the Office of Privacy Protection in the State of California's Office of Consumer Affairs, which focuses on privacy and identity theft protection for California citizens. Additionally, I have served on the Los Angeles District Attorney's Office Task Force on Identity Theft, which sponsored legislation to help victims of identity theft, and assisted law enforcement in the prosecution of this crime. As an advisory board member to the non-profit consumer advocacy programs, the Privacy Rights Clearinghouse and the Identity Theft Resource Center (San Diego, Ca.), I am privileged to consult with Directors Beth Givens and Linda

Foley regarding identity theft cases, research, protection for consumers and companies, and proposals for legislation.

My own identity was stolen (in 1996) by an impostor who paraded as an attorney robbing me of my profession, my credit and my peace of mind. She obtained over \$50,000 using my name, purchased a red convertible Mustang, and even caused me to be threatened with a lawsuit by a rental car company for the car that she leased and damaged in an accident. It took me almost a year to clear my records and regain my credit and my life. I later learned that while working as a secretary, my evil twin (who I never met) accessed my credit report with all my personal and financial information on-line from a subscription service. From that arduous nightmare, I gained great insight into the tribulations that victims endure. Since that time I have personally assisted myriad victims across the country. I have had the privilege of testifying before several legislative bodies and have advised many national corporations on how to protect their clients, customers, vendors, employees and their company from great challenges of identity theft.

First I am grateful to this honorable committee for focusing on the growing problem of privacy and security with regard to the Internet. Your desire to expose these issues and educate our citizens deserves commendation. I am also thankful to this esteemed panel of witnesses who will bring light on these problems and help to create solutions so that we may better protect our personal and confidential information while using file sharing and other technologies on the Internet.

You've asked that I concentrate my testimony in the following areas:

I. Provide you an overview of how your identity can be stolen through the acquisition of your personal information.

II. Document examples of identity theft cases which have occurred with the use of personal identifiers.

III. Suggest ways in which computer users and ordinary citizens can protect themselves from the threat of identity theft, which may be posed by the vulnerabilities of peer-to-peer sharing and other Internet technologies.

I. HOW YOUR IDENTITY MAY BE STOLEN THROUGH THE ACQUISITION OF YOUR PERSONAL INFORMATION

In our data driven society your personal information is readily transferred across the nation in a nano-second through networks and on the Internet (whether or not you are a computer user). Your personal information, worth **more** than currency itself, can be used to apply for credit cards, credit lines, mortgages, cell phones, insurance, utilities, products and services etc. all without your knowledge. A fraudster can do *anything* you can do with your identifying information- and worse- even do things you *wouldn't* do such as commit crimes or engage in terrorist activities.

A. WHAT IS IDENTITY THEFT AND WHAT IS THE MOTIVATION?

\ Identity theft is the use of your personal identifying information such as your name, social security number, address, birth date, unique passwords, even biometric information, (usually the key to identity door is the social security number) to commit some type of fraud for one of the following benefits to the fraudster:

1. **Financial Gain**-This includes credit, loans, employment, health care, insurance, welfare, citizenship, other governmental and corporate benefits- and anything that has a dollar value. The fraud may take place in many jurisdictions, and purchases can be made by phone, fax, on-line or in person. Usually, the perpetrator can buy or “legally” obtain a driver’s license, create checks on a computer with the victims’ name, obtain or buy other identity documents including medical cards, credit cards, passports, etc.

2. **Avoiding Prosecution-** A criminal commits crimes in the real world or virtual electronic world, or terrorist acts using the name and identifying information of another person. Often the perpetrator also commits financial fraud as well to supplement her income.

3. **Revenge** - One can remain "invisible" by stealing an identity to hurt another person. This type of fraud may occur between ex-spouses, former business partners, ex-employees, disgruntled staff or angry customers. We also see this type of fraud committed in businesses where one business owner will want to ruin the reputation of another. This is tantamount to business identity theft.

B. HOW DOES THE FRAUD OCCUR?

Stealing your identity for financial gain is the most common motivation for a thief. The Federal Trade Commission's Report on Identity Theft (12/02) www.consumer.gov/idtheft) summarized the data received from consumers regarding identity theft complaints. They found that of all reported identity fraud complaints (279,134 in their data base as of 12/02), credit card fraud comprised 42%, utility fraud comprised 22%, bank fraud 17%, Employment fraud 9% Fraud loans 6% and government benefits 8%. Almost a quarter of the consumers complaining experienced more than one type of fraud. It's also important to note that many victims are not still not aware of the FTC's Clearinghouse. The clearinghouse was instituted as a result of the Identity Theft and Assumption Deterrence Act of 1998. I was privileged to testify at the Senate Hearing to support the bill establishing this act which also instituted identity theft as a crime against the consumer victim and set forth criminal penalties in 18 USC Section 1028 (a7) Although victims are starting to become more aware that the Federal Trade Commission provides helpful resources and takes complaints (toll free 877 ID Theft or www.consumer.gov/idtheft) through law enforcement and credit grantors referrals, many don't complete a complaint form. Some victims tell us that they know that the FTC cannot take their individual case, or personally assist them (other than to provide excellent resources like affidavits, referrals, steps to take), and they are reluctant to reveal more of their private information.

The scope and extent of the problem of identity theft and number of victims is still unclear, although the numbers are increasing. In 2002 the FTC received 162,000 complaints of actual victims. In 2001 Trans Union (one of the major credit reporting bureaus) reported 3500 calls a day to its fraud hotline (not all were victims, some had lost their wallet or were aware of a security breach and were potential victims). They also reported that they received 85,000 calls a month to their fraud hotline in 2001. The epidemic of identity theft is growing. Our experience and the research shown by the Government Accounting Office Reports (www.gao.gov) the FTC at www.consumer.gov/idtheft), the Privacy Rights Clearinghouse (www.privacyrights.org) and others is that most victims' information is acquired very easily. Most often the information is stolen **off-line**; however the data is quite often used on-line and by mail to apply for credit, services, and products. For the savvy impostor, the Internet and mail provide a safer refuge to commit fraud rather than face-to-face contact where one could be confronted and apprehended.

Because of the vast ways in which personal information can be obtained, it is critical to note that most victims (according to the Federal Trade Commissions 2002 Report-**72%**) have ***no idea*** how their information was accessed unless a wallet was stolen or lost or if a family member was the impostor. Most identity theft takes place without the knowledge and beyond the control of the victim. And many who fall prey don't find out for months or even years until they are denied credit or employment, threatened by collection companies, or arrested for a crime they didn't commit.

The newest May 2003 CALPIRG (California Public Interest Research Group) study "Policing Privacy: Law Enforcement's Response to Identity Theft" (see pages 10-12 www.calpirg.org/reports) lists the top common sources of identity theft:

(I have listed them for you from the study, but added my own comments explaining what they are)

1. **Mail Theft** –Pre-approved offers, convenience checks, documents from banks and financial and insurance institutions containing social security numbers, account

numbers and other critical data provide a goldmine for potential impersonators. (68% of law enforcement interviewed named mail theft as a top concern leading to identity theft)

2. **Dumpster Diving** Thieves search through garbage in offices, on the street, and at commercial locations for information. Several states including California now require commercial businesses to shred or completely destroy personal information prior to discarding it to protect customers. Consumers are advised to purchase home shredders and shredding software to protect themselves.
3. **Unscrupulous Employees** - Insiders with access to information off-line and on line have a “candy store” of opportunities to commit identity fraud. For example, we know of many instances of car salesmen, “dirty” employees working for credit reporting agencies, and realtors selling credit reports. There were instances of employees from the Social Security Administration selling social security numbers, bank employees using passwords to deplete customer funds, insiders stealing information from personnel and customer files to sell or use themselves to obtain credit and services. Pilfering can be accomplished through trash inspection, stealing hard copy documents or copying of files from a computer. A couple of years ago, in Detroit, several General Motors executives became victims of identity theft when a temporary employee obtained printouts of lists of personal information of the important staff. Another recent example is the theft by an ex-employee of a software company who used passwords previously accessible to him (and the company didn’t change the passwords after he left) to obtain credit reports of customers of Ford Motor Credit. He sold the credit profiles of thousands of potential victims. Your credit profile –especially one for commercial vendors have all a fraudster needs to steal your identity.
4. **Stolen/lost wallets-** This source of information loss is one of the few ways in which consumers may trace the theft back to the source. Although not mentioned by the

Calpirg study, lost, stolen or never received credit cards, convenience checks and pre-approved offers are another great source for criminals to commit financial fraud.

5. **Internet Fraud** (and computer access fraud.) There are numerous types of fraud that can begin with the accessing of information from a computer whether or not the machine is networked or connected to the Internet. A stand-alone computer can be entered if there is no password protection and sensitive non-encrypted files can be copied or removed. Many computer users keep personal information including passwords and confidential financial documents on the computer with little protection. Of course, while on a network or internet- and especially with wireless connections, hackers can intrude and take what they find un-noticed. Also, fraudulent e-mails, fake websites copied to look like real trusted sites, can gather your information through deception. However many times information may be hacked through security holes in trusted software. The most current example is of this is the Microsoft "Passport" flaw exposed last week. The system problem allows an attacker to access vital confidential personal data passwords, credit card information, etc. Peer to Peer file sharing if used incorrectly or if corrupted can permit entry by unsavory file sharing characters to access sensitive files with personal information. We've all seen the news of entire personnel files, student profiles, and credit card customer files stolen by hackers creating privacy invasions and worse yet, identity theft. A recent example is the theft of several hundred thousand health records (including the Social Security numbers) of Veterans in Arizona. Recently VISA and MasterCard customer information was hacked from a company that processes credit card transactions and it is believed that several hundred thousand files were compromised. With these types of security breaches, computer users are powerless to do anything to protect themselves prior to the intrusion.
6. **Burglary- Theft** from houses, cars, businesses of hard copy documents, faxes, e-mails, computer files, etc. Data collected on a personal level would be billing statements, bank documents, loan applications, utility bills, investment reports, credit

card bills, insurance statements, and credit reports. Business records could be client and customer files and profiles, trade secrets, data bases, financial records, computer hard drives, etc.

7. **Friends, Relations-** Unfortunately, intimate friends and family have access to our personal information or places in which we keep that information. The elderly, ill or very young are most susceptible to caretaker abuse. The trusted individual may have access to check writing, credit cards, personal information, etc. This is especially tragic since a victim may not wish to prosecute a family member, and therefore may be left with the financial burden of the fraud charges.
8. **Phone Scams:** Fraudsters induce victims to reveal personal information through pretext calling- pretending to be your bank, or a governmental agency in need of your personal information.
9. **Unethical Use of Public Documents** –Birth Certificates, Death Certificates, Marriage Licenses, etc. all are public records and easily attainable on the Internet through governmental agencies, on-line information brokers, or even in person. These documents display social security numbers and other personal identifiers including mother's maiden name. (California recently passed a law requiring that public records which contain the social security number be restricted (information redacted for public disclosure) except for use by "need to know" persons.
10. **Shoulder Surfing-** Potential imposters watch for vulnerable computer users, ATM and other machine users to ascertain passwords and other information to steal.
11. **Medical Cards** –Many insurance carriers still use the social security number as the key to the system. Other personal and confidential data is also readily available for use by prying eyes at pharmacies, doctor's offices, hospitals and clinics.

**C. OTHER MEANS OF APPROPRIATION OF PERSONAL AND
CONFIDENTIAL INFORMATION NOT REPORTED BY CALPIRG LAW
ENFORCEMENT STUDY ABOVE:**

1. Government Data Sources Revealed- There is still several governmental agencies both state and federal that requires the display of the social security number in plain view. This is true for military service and veteran health care. Several states still use the social security number as the Driver's license number, which must be shown for identification purposes, for travel on airplanes, when cashing checks, and in other public matters. The social security number must be displayed on payroll checks in California and other states (a California bill is pending to eliminate this requirement). The State of California Peace Officers Standards Training for all police requires that the social security number be displayed and indicated for the peace officers to continue employment. Also many state colleges require that the social security number be the key identifier and be displayed for grades. There are pending bills in the California legislature to cure these problems.

2. Personal Information Sold By Financial Institutions

In GAO testimony of 4/14/02, regarding **Identity Theft: Available Data Indicate Growth in Prevalence and Cost**, the Director, and Justice Issues indicated:

“Another potential source of personal identifiers for identity thieves is the personal financial information sold by financial institutions to non-affiliate third parties” Under the Gramm-Leach-Bliley Act of 1997 (GLB), a financial institution can sell your private financial data unless you respond to their “opt out” privacy notices which must be sent annually which inform a consumer of the privacy policies of that institution. There is presently a state bill in California (and also a pending Ballot Initiative) that would require that financial institutions apply the “opt in” standard, which would allow customers to prohibit such disclosure without express prior permission.

3. Stealing Information Regarding Internet Technologies Such As Peer File Sharing

As you can see from the information above, your personal information can be stolen in a variety of ways-most of which are very easy, and don't even require any high tech instruments. In this data profiling society, our personal and business information is available everywhere! But this doesn't mean that we should ignore the vulnerabilities of peer-to-peer file sharing. The Internet and software programs that contain security flaws, or require a great deal of understanding to use effectively – pose a threat to non-techies who want to use the new technology. Unsophisticated users of P2P File sharing may be sharing much more than they intend to and unintentionally enable a “peer” to become an identity clone. Since most victims don't know how their information is stolen to commit identity theft, it is feasible that users of these technologies who accidentally share files that contain confidential and personal information- could be subjecting themselves to the potential identify theft. One of our witnesses today, Nathan S. Good wrote an article “Usability and Privacy: A Study of Kazaa P2P File Sharing”- This study is helpful in understanding that fatal mistakes by unaware users could allow someone to get into unencrypted files with sensitive information. If you keep passwords, credit card numbers, financial information, software programs with financial information for banking in un-encrypted files (or poorly encrypted files) and you haven't understood how to make certain that *only* your designated file for sharing is open to share, you are vulnerable to exposing your information. Just as in many other programs that enable you to network, bank on-line, share e-mails, purchase with ”passports” or use other profiling software, there may be security flaws that invite a hacker to appropriate confidential files from your hard-drive. Hacker attacks and security breaches are well known to companies and governmental websites as well. You have little control over the security flaws, but you do have control over the steps you can take to protect yourself while using technology. Steps to minimize your risk will be addressed in the later section of the testimony.

II. DOCUMENTED EXAMPLES OF CASES OF IDENTITY THEFT USING PERSONAL INFORMATION

A. Examples of Financial Identity Theft:

1. John is a recent widower. When his wife died of cancer at age 35, (leaving him with three young children, he began receiving collection calls from credit card companies, a computer manufacturer, and a cell phone company for the items and services allegedly purchased by his deceased wife after her funeral. He suspects that the imposter got the information from the death certificate which has the social security number and birth date on the document. This could have been obtained in the funeral home, from public records off line or on line, through the social security administration, from an Internet information broker, or any number of places.

2. Sidney, a wealthy retired executive learned that his identity was stolen many months after he and his wife purchased a new home. His loan application, with his 3 in one credit report attached, revealed his credit score, his checking, savings, and investment accounts, social security number, and all necessary information for an impostor to become Sidney. He believes his masquerader had gotten a copy of Sidney's loan application through his broker's laptop computer (which also had his downloaded credit report) and opened new credit card accounts, purchased computers, electronic equipment, furniture, rented an apartment, obtained utilities, etc, stealing almost \$100,000.

3. Robert is a high tech computer consultant who normally encrypts all sensitive data on his computer. Unfortunately, his resume was not stored in an encrypted file. He suspects that somehow his impersonator accessed his computer through a network and copied his resume. The fraudster used the vitae as his own to obtain a well paying job with the government. When Robert applied for the same job- he was shocked to find out another person with his name and credentials was already hired- the agency thought he was the fraudster.

B Examples of Criminal Identity Theft

1. George, a disabled veteran living in Colorado was suddenly denied his disability payments, and hit with a large IRS bill for the income that his impostor had earned working under his name in Tennessee. Upon further investigation, we learned that George's impostor had also established a criminal record in yet another state and there was a warrant for George's arrest.

2. Debbie signed up for e-mail and Internet access with a reputable Internet Service Provider. She received e-mail from her provider asking her to give her personally identifying information, including her social security number, to renew her account, she later learned that she and many other people had responded to a false e-mail set up to look like her provider. Months later she received collection calls and when stopped for speeding one night she was nearly arrested for outstanding warrants issued in her name in another state.

3. Tom was laid off from a high paying job in the medical industry. He had great recommendations and felt sure he would be rehired. For two years he was denied

position after position after each company had done a background check. Finally Tom hired a private investigator who showed him that his criminal background included 2 DUI's and an arrest for murder. None of which belonged to him. He learned that an on-line information broker continued selling this erroneous information even after he corrected it with the Sheriff.

C. Examples of Identity Theft for Revenge

- 1. Dan was trying to get joint custody in divorce proceedings. His estranged wife somehow was able to access his e-mail accounts and passwords and send herself fraudulent e-mail messages from him threatening to harm her and kill the children.*
- 2. The first cyber stalking case prosecuted in Orange County, California turned out to be identity theft. A computer expert was angry when a woman he liked shunned his advances. He proceeded to go online to a chatroom and pretend to be her- stating that she has fantasies of being raped. He gave out her telephone number and home address. The woman didn't even own a computer. When several men appeared at her door to share her fantasies, she was terrified and called the police.*
- 3. The Sept 11, 2001 terrorists had opened 14 accounts at a Florida bank, using false social security numbers and other documents. They obtained credit cards, apartment units, leased cars, and fraudulently charged airline tickets. They not only did this for revenge against our country- but also they committed financial theft to avoid being caught or prosecuted.*

The above cases demonstrate how identity theft can take many forms. Often the victim can only guess how his information was obtained. The assaults against these victims caused great anguish and negatively impacted every aspect of their lives. The time spent trying to regain their lives, the damage to their reputation, and the out of pocket costs were minimal compared to the tremendous emotional turmoil these people endured. The purpose of showing you these examples is to help to understand why it is so important to educate our citizens, support law enforcement efforts, encourage best business practices with regard to Internet technologies, and pass laws which hold the financial industry accountable to verify and authenticate before issuing credit to possible identity thieves. (Please see S. 233 The Identity Theft Prevention Act of 2003).

III. WHAT COMPUTER USERS CAN AND CANNOT DO TO PROTECT THEMSELVES FROM IDENTITY THEFT WHEN USING PEER TO PEER FILE SHARING

What can computer users do to protect them while using these technologies and other Internet or Network programs? The Internet provides an opportunity for increased knowledge, entertainment, and global communication. At the same time it provides a free forum for dangers including unsavory hackers, attackers, child molesters, and fraudsters. Since I am not a computer expert, but use my PC everyday for business, education, and communication, I can suggest what I as a specialist in identity theft to my friends and clients.

1. **RESEARCH ANY PROGRAM BEFORE INSTALLING IT.** As my own computer consultant warns me daily, before you put a new program on your computer, find out everything about the program that you can, and learn what risks there are in using it. Take every precaution that the program advises. And if you aren't highly technical, get some help in deciding whether to even use a program at all. If you decide to use a program, look first to the security and privacy actions to take. This applies to all software you purchase or download.
2. **LEARN HOW TO SAFELY STOP SHARING YOUR FILES AND HOW TO BLOCK UNWANTED FILES FROM ENTERING YOUR COMPUTER.** If you aren't sure what you are doing get on the website of the software company and get some technical support either by e-mail or by phone to help you correct any miss-configurations you have made. Also have them double check that you have made the right choices. When downloading- don't designate more than one folder for file sharing, and check to see in "tools" if you have inadvertently checked more than one file- if so – immediately unselect the files you don't want to share. If you have problems, delete the program until you know how to limit the shared folders.
3. **IF POSSIBLE, WHEN USING PEER-TO-PEER FILE SHARING AND THE INTERNET, USE A COMPUTER THAT DOESN'T STORE SENSITIVE INFORMATION ON IT.** This may not be feasible because of the costs. But some companies and individuals have a separate computer for Internet use.
4. **PASSWORD PROTECT AND ENCRYPT YOUR SENSITIVE FILES,** Make sure that you are carefully protecting information that could be used to steal your identity. Don't tell anyone your passwords and change them from time to time- especially when an employee who had access, leaves your business. Also don't store passwords on your computer.
5. **DON'T PUT ANY CONFIDENTIAL INFORMATION IN YOUR E-MAILS UNLESS THEY ARE ENCRYPTED.** This is important whether you file share or not. E-mail is like a postcard. Your e-mails at work are not confidential and may be reviewed by your employer. There is no expectation of privacy for e-mails.
6. **BE CONSCIOUS ABOUT WHAT INFORMATION YOU SHARE IN YOUR FILES, AT WEBSITES, IN CHAT ROOMS AND IN E-MAIL.** Just because you're asked to share information, doesn't mean it is safe. Consider what could be done with the information you disseminate, and then reconsider.
7. **READ THE PRIVACY POLICIES OF THE WEBSITES YOU DEAL WITH.** If they share your information for marketing purposes, think twice about providing it, since it can be aggregated and sold and used to profile you. Someone getting that information may become your identity clone.

8. MAKE SURE YOU HAVE VIRUS PROTECTION ON YOUR COMPUTERS. Update it often.

9. DON'T ASSUME THAT YOU ARE ANONYMOUS. Remember there is online tracking and monitoring when you use the Internet. Install reputable spy wear and find out about other security measures to take.

10. USE A HARDWARE FIREWALL WHENEVER POSSIBLE. Be especially careful if you have a wireless connection to set up firewalls otherwise you are opening up your entire system to strangers and all your files can be accessed.

For more tips and security suggestions about protecting your privacy and identity on-line see **Fact Sheet 18: Online Privacy at the Privacy Rights Clearinghouse** at www.privacyrights.org. Also visit the Electronic Privacy Information Center at www.epic.org. There are additional resources listed on both websites to educate the novice as well as the most seasoned computer guru.

OTHER IDENTITY THEFT PROTECTIONS MEASURES:

Here are the top four protection measures we suggest:

1. Get a copy of your credit reports at least twice a year. Carefully scrutinize all information and correct all errors, including the inquiries. If something looks strange, call and write to the creditor and place fraud alerts on the credit profiles of the three major credit reporting agencies. If you monitor your reports and fraud accounts are opened, at least you will minimize your losses with early notification. Does your own background search on yourself once a year to see if any fraudulent criminal activity appears?

2. Don't give out your social security number unless required by law. Don't carry it with you and if it is on your health care cards, make a copy redacting the first 5 numbers and carry only the copy with you. Carry as little information about you as possible in your wallet. Don't submit to the use of your biometric information (fingerprint, iris scan, etc) unless required by law and you understand the purpose for which it is collected, how it will be maintained, the secondary use if any, the safeguards ensuring its accuracy and security and the place to contact if a problem arises.

3. Guard your personal information with great caution. Don't give out information at retail stores, on warranty cards, when a company *calls you* on the phone, or on the Internet. Don't keep personal information on your computer if it is accessible on the Internet. Shred all documents that you are discarding, including utility bills, check statements, old wills and trusts, **anything** with personal and financial information.

4. When dealing with others in a trusted position, such as a caregiver, or a trusted advisor, make sure you check references, licenses, and other background information. Share as little personal and financial data with this person as possible, and don't give them responsibility to

manage your assets without your approval- don't give out your ATM VISA pin number or allow them to sign checks for you. The less access to your financial and personal data the more secure your identity.

THE MYTH OF PREVENTION OF IDENTITY THEFT

This testimony described many ways that your information could be accessed and used for financial gain or a criminal purpose without your knowledge or control. When I became a victim, my impostor had accessed my credit report from a law office subscription service with a re-seller of credit profiles. She pretended to be a private detective declaring under penalty of perjury that she had a permissible purpose to obtain my credit report. I had no way to prevent this crime from happening, since the information was not within my control. The majority of victims cannot prevent this crime. Therefore, offering computer tips and offline suggestions on how to “*avoid*” identity theft would be misleading. Although we may educate ourselves as to vulnerabilities of the Internet and Peer-to-Peer File Sharing, and protect our information off line as well, if someone wishes to steal our identity, the information they need is within their reach in many places and it will un-avoidable. If you are victimized by identity theft go to www.identitytheft.org; www.consumer.gov/idtheft www.privacyrights.org and www.idtheftcenter.org for many pages of free information to help you deal with the ordeal of regaining your identity.

As computer users and concerned citizens, we must educate ourselves, research and understand the programs and technologies we use, and guard our information as best as possible, I urge this committee to take notice that we should **not** give any false sense of security to anyone with regard preventing identity theft. We cannot guarantee anyone that if they don't use Peer-to-Peer File Sharing, they will be safe from identity theft. No matter where a criminal gets your information, it can only be used for financial gain if the creditors and other businesses are not cautious about verifying and authenticating your identity.

For that reason, I have listed below suggested steps that should be taken by governmental and commercial entities to prevent financial identity theft.

IV. PROPOSED ACTIONS TO PREVENT IDENTITY THEFT

- 1. Both governmental entities and private industry should limit the use of the social security number since it is the key to identity theft for financial fraud.**

As a member of the advisory committee in the Office of Privacy Protection in the California Office of Consumer Affairs, I had the privilege of assisting in the development of the recently issued “ **Recommended Practices for Protecting the Confidentiality of Social Security Numbers**” (July 25, 2002 www.privacy.ca.gov). This document should be considered by both public and private sector entities to protect all consumers.

- 2. Destruction of Confidential Information**-Governmental Agencies and Private Industry should be required to completely destroy personal information that they are discarding by

shredding, burning or whatever means is necessary to protect the information from dumpster diving.

3. Governmental and Private industry should be required to truncate credit card numbers – No company or entity shall print more than the last 5 digits of a credit card number or account number or the expiration date upon any receipt provided to a cardholder.

4. Security Breach Notification Governmental Agencies and Private industry should be held accountable to timely notify all employees and or clients or customers of computer security breaches which have exposed their personal identifying information.

5. Departments of Motor Vehicle Licensing- Bureaus should establish more stringent monitoring and matching of duplicate licensing and new licenses. A photo ID and a fingerprint could be matched. Rather than developing a “national ID” with various forms of biometric information, credit cards and other unnecessary information which would complicate the process, this national driver’s license would have a national data base to help deter interstate identity theft.

6. Law enforcement agencies should be required to take a report in the jurisdiction where the identity theft victim lives. Such report should enable the victim to list the fraudulent accounts so that this report could be sent to the credit reporting agencies to comply with their policy of blocking the fraud accounts upon receipt of a valid law enforcement report.

7 Law enforcement agencies should be provided funding for task forces in all major metropolitan areas to include the Secret Service, the Postal Inspector, the Social Security Inspector, the FBI, INS, State Attorney General and local law enforcement to collaborate in the investigation and prosecution of these crimes.

8. Local law enforcement agencies in conjunction with the judicial system should assist victims of criminal identity theft in other jurisdictions within a nation wide coordinated system. So a victim of criminal identity theft in California whose impostor is in New York could be declared innocent in New York as well as California. This would entail a national database of the criminal information and fingerprints. It would contain the order of the true person’s fingerprints for comparison with the fingerprints of the impostor-criminal in New York. The court would enter a declaration of factual innocence and any warrants for the victim would be dismissed. All databases would be corrected so that background checks would not show the victim as having an arrest or criminal record.

9. Increase penalties for repeat identity theft perpetrators or for “aggravated identity theft” and for those who commit identity theft for the purpose of committing terrorism.

10. Set up State and Federal Offices for Privacy Protection- There should be a federal office of privacy protection as well as state offices. The office of privacy protection should

institute an ombudsmen office to assist the elderly and limited English speakers to resolve identity theft problems.

10. Credit Reporting Agencies:

a. Since most victims do not have notice of the identity theft until they re-finance, apply for a loan, or are contacted by a creditor, the statute of limitations to file a law suit against a credit reporting agency should begin within 2 years of the date at which they *discover* or should have known of the fraud.

b. To assist in the monitoring of credit reports, consumers should be entitled to a free credit report at least once a year in every state.

c. Credit reporting agencies should provide to consumers, upon request, an exact copy of the credit reports that vendors and creditors receive since often they are different and the consumer credit report often shows different account information, which causes difficulties for victims in clearing their credit.

d. Consumers should be able to put a complete freeze on their credit reports in order to prevent identity theft. This would enable the consumer to prevent their credit report from being accessed by a creditor without the specific authorization of release. It would be impossible for an impostor to apply for credit if there were a freeze on the file. The consumer would have the right to release the file when he so desires by a password or pin number. This type of legislation recently became law in California.

e. Credit reporting agencies should be required by law to block all fraud including the fraudulent inquiries upon the receipt of a valid law enforcement report (local police, DMV investigators, Secret Service) listing the fraud accounts. The burden then shifts to the creditors to prove that the accounts are not fraudulent. This is presently law in California and should be codified nationwide. Under this scenario the victim of fraud is innocent until proven guilty instead of having the burden of proving innocence.

f. Credit reporting agencies should provide names, addresses and phone numbers of the companies who accessed the consumer's credit report – (inquiries) with the issuance of a consumer report so that potential victims could verify the permissible purpose.

g. Credit reporting agencies should notify a consumer by e-mail or First Class mail when his/her credit report has been accessed. The agency should be allowed to charge a reasonable fee for this service.

h. To provide better enforcement, the Fair Credit Reporting act should be amended to allow for class action lawsuits for violations of the act by creditors and credit reporting agencies.

I. Credit reporting agencies should set up hotlines with live persons to talk to regarding identity theft. The same employee in the fraud department should be assigned to a particular victim.

j. Since many states are providing more privacy safeguards and better identity theft protection for their citizens than federal laws provide under the Fair Credit Reporting Act, the sunset provisions of federal pre-emption should not be re-instated. Several states like California have influenced other states and the federal government to more carefully guard our confidential information from the identity impostors.

11. Banks and other Creditors should be held accountable for protecting consumers and others from identity theft.

a. The fraudsters' most critical need in committing identity theft is to change the victim's address to the impostor's address or mail drop. Creditors either extending credit to a new account or upon being asked to change the address on the account is required to verify the address change if it is different from the address on its records or the address on the credit report. The creditor should be required to send a notification and confirmation to the former as well as the new address. Also if the creditor receives a request for an additional card it should notify the primary cardholder.

b. Creditor's who issue credit to an impostor after a fraud alert is placed on a credit profile, should be held liable and assessed a fixed penalty of at least \$1000 per occurrence or actual damages which ever is greater.

c. Upon receiving notification of fraud by a victim of identity theft, a creditor should be required within 15 days to provide copies of all billing statements, applications and other correspondence to the victim. The victim may be required to pay reasonable copying costs.

d. Credit grantors should compare and match with the credit report for verification purposes, at least four pieces of personal information that would identify a consumer applying for credit.

e. Credit grantors should utilize their financial discrimination programs to identify changes in spending habits so they could intervene early and notify consumers of possible fraudulent activity before it gets out of hand.

f. Creditors should not be allowed to send "convenience checks" without a request by the consumer.

g. Credit grantors should not be allowed to send pre-approved offers of credit without the request of the consumer.

12. Regulation of Information Brokers

a. Information brokers should be subject to the Fair Credit Reporting Act as defined by statute so as not to shirk their duty to maintain accurate records.

b. Employers or others who order background checks on a consumer should be required to provide a copy to the consumer upon receipt whether or not the consumer report was used to hire a prospective employee or any other purpose.

Privacy, Security, and Identity Theft Conclusions

Personal, confidential, and financial information is a valued commodity in our society. Marketers and the financial industry buy transfer and sell your aggregated personal profiles which include your income, credit worthiness, buying, spending, traveling habits, health information, age, gender, race, etc. Facts about our personal and financial lives are shared legally and illegally without our knowledge or consent – on-line and off-line everyday. Privacy protection in the age of data collection is really about limiting access to our records, rather than keeping the information secret. . The only power you have is to educate yourself as to your risks and to the potential dangers of privacy and security invasions. This loss of control over the dissemination of your information has led to the epidemic of identity theft. It's wise to research the perils posed by the Internet, Peer to Peer File Sharing and similar technologies and arm yourself with knowledge, security measures and careful strategies. It's important to expose security flaws in software to the media and Congress, so that companies will make security a top priority and make their programs easier to use. But all this will not stop a fraudster who steals your information from a source outside of your control such as your doctor's patient files, or your accountant's fax machine, your HR department's computer at work, or from the trash behind your bank or insurance company.

To avert *financial* identity theft, the burden must be on the creditors who are in the unique position on the front end, to take precautions, require verification, and refuse to issue the credit card or loan to a fraudster. The financial industry has the power prevent a potential identity theft *before* the impostor can establish a parallel “shadow credit profile”. To limit criminal identity theft, law enforcement has the power to protect potential victims. When a perpetrator is apprehended and gives a victim’s name, his fingerprints and mug shot should always be taken, and the information should be stored securely for viewing, in a safe centralized, national law enforcement data base. That way, if a victim learns of a warrant for his arrest in another state, his photo and finger prints can be compared with those of the impersonator in his own state, and his name can be cleared effectively and expeditiously. With a greater emphasis on precluding the facilitation of this crime at its inception-*before* the credit is wrongly issued, there will be a greater trust in law enforcement’s abilities to reduce fraud, and the financial industry’s commitment to protect its customers.

Thank you for the opportunity to share these concerns and suggestions with this Honorable Committee.

Mari J. Frank, Esq.

Attorney, Mediator, Privacy Consultant
28202 Cabot Road, Suite 215
Laguna Niguel, California 92677
Phone: 949-364-1511
Fax: 949-363-7561
E-mail: contact@identitytheft.org or Mari@MariFrank.com
www.identitytheft.org
www.MariFrank.com
